⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭61－108272

⑤1Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和61年(1986)5月26日
H 04 N 7/16		7013－5C	
7/167		7013－5C	

審査請求　未請求　発明の数 1　（全7頁）

㊹発明の名称　有料放送方式

㉑特　願　昭59－229018
㉒出　願　昭59(1984)11月1日

㉒発明者　森田　博幸　深谷市幡羅町1－9－2　株式会社東芝深谷工場内
㉒発明者　国井　満雄　深谷市幡羅町1－9－2　株式会社東芝深谷工場内
㉑出願人　株式会社東芝　川崎市幸区堀川町72番地
㉔代理人　弁理士　則近　憲佑　外1名

明　細　書

1. 発明の名称　有料放送方式

2. 特許請求の範囲

放送局側において有料放送番組に対応した番組種別情報を発生する番組種別情報発生手段と、

前記有料番組放送を加入者が契約したことを示す契約番組種別情報発生手段と、

前記有料放送信号に対してスクランブルを行なうための鍵情報を発生する鍵情報生成手段と、

前記鍵情報、前記番組種別情報及び前記契約番組種別情報を送出する送出手段とを有し、

受信側において前記番組種別情報、及び前記契約番組種別情報を抽出する抽出手段と、

前記鍵情報を抽出する鍵情報抽出手段と、

前記契約番組種別情報と番組種別情報との比較を行なう比較手段と、

この比較手段によって前記契約番組種別情報と番組種別情報との対応が検出されない場合、表示器を駆動して加入者が当該有料番組に対し未契約であることを表示する表示手段とを有したことを特徴とする有料放送方式。

3. 発明の詳細な説明

〔発明の技術分野〕

この発明は、例えば放送衛星等を用いた空中線或は伝送線を介するCATVに代表される有線形態で映像、音声、データ、図形情報をサービスする形態において視聴を契約した加入者のみにサービスを行なう有料放送方式に係り、特に加入者が番組予約をし忘れた場合等で受信できないとき機器の故障ではなくディスクランブルのための鍵が生成されていないことを示し得る有料放送方式に関する。

〔発明の概要〕

この発明に係る有料放送方式では、例えば第1図に示すように放送局側100では、データメモリ60に有料番組の種別を示す予約ティア情報(Ti)、及び有料番組に対してスクランブルするための鍵情報が格納されており、この鍵情報を用いて乱数発生器10で乱数を発生させ有料放送信号を排他的論理和回路210でスクランブルする。また、デー

タメモリ70には加入者識別符号(ID)に対応して当該加入者が契約している場合には該当契約有料番組の種別を示す予約ティア(Ti)として格納される。

加入者側200では予約ティア(Ti)は鍵抽出回路223で抽出され、受信ティア(Ti)は鍵抽出回路228で抽出され、両ティア(Ti)は比較器229で比較される。比較結果が両ティア(Ti)が一致しない場合にはＣＰＵ300は表示器400を駆動する駆動々作を行なう。この表示駆動によって加入者に対して未契約であることを知らせる。

また、この場合、制御回路230は復号器231の復号動作を停止させ乱数発生器220での復号のための乱数の発生が停止される。

〔発明の技術的背景とその問題点〕

近年、新放送メディアの発達にともない、テレテキスト、静止画放送、高品位テレビジョン放送、デジタル信号による多チャンネル放送が可能となってきている。このような放送メディアの高度化により放送番組の伝送種類も多岐にわたってきている。

(3)

化された情報を平文化して復号を行なう。

このような有料方式においては上記したように放送局側に対する番組予約は公開鍵を用いて行ない放送局側で課金に対する検査を行なった後に暗号化された情報を平文化するに必要な情報が加入者側にダウンロードされる。

上記有料放送方式においては、予約番組情報であるティア(Ti)を放送局側に登録することで予約がなされ、有料放送の視聴を可能にする鍵情報が当該加入者に対して設定されて当該有料放送に対する加入者の視聴を可能にする。このため予約動作によってスクランブルを解くため鍵情報が設定されないと、加入者は当該有料番組の視聴ができない。この場合、加入者の予約（契約）し忘れによる原因か或は機器の故障原因のいずれの原因により加入者が視聴できないのか加入者には判別できない。

そこでスクランブルを解く為の鍵が加入者側で得られない場合には加入者にこれを知らせ、故障によって視聴できないのではなく予約のし忘れ時

(5)

そして、放送側においては特定番組に対して課金を行ない放送局側と契約を行なった特定の加入者以外の加入者に対しては伝送信号に対して撹拌を与え、いわゆるスクランブルを行ない視聴を阻止し、契約加入者に対してはこのスクランブルを解除することによって視聴を可能にする有料放送が有料番組に対して行なわれる。

この場合、有料放送方式において加入者が有送番組を予約するには識別符号(ID)とともに所望の番組を予約する訳であるが、実際の加入者以者の名義で不正予約を防ぐ意味において当該契約者固有の識別信号(ID)を放送局側に告知することを番組予約時に行なわせるシステムが採用される。即ち、識別信号(ID)、及び予約対象番組を示す公開鍵であるティア(Ti)と呼ばれる情報で放送局側に番組予約をし、放送局側ではこれらの公開情報を秘匿情報に変換してどの加入者が契約したかの情報及び信号に対するスクランブルを解くための情報の両者を秘匿する。この秘匿情報は加入者側に送られ、この秘匿情報より復号化鍵を生成し暗号

(4)

によって加入者に上記鍵が与えられていないことによることを知らせる必要がある。

即ち、予約を完了してない番組を加入者が選定したときには未予約であることを加入者に認知させることが望まれる。

〔発明の目的〕

この発明は上記の点に鑑みなされたものであり加入者の予約作業によってスクランブルを解くための鍵が当該加入者に与えられないときには、未契約である旨を加入者に認知させることのできる有料放送方式を提供することを目的とする。

〔発明の実施例〕

以下、この発明の一実施例を図面を参照して説明する。

第２図はこの発明に係る有料放送方式の一実施例を示す回路図である。この第２図に示す回路によって放送信号に対するスクランブルよって伝送信号に対する暗号化がなされるが、課金対象となるデジタル放送情報は入力端子ＩＮに印加される。

この放送情報は有料放送としてスクランブル処

(6)

理され加入者に対してのみ復号がなされるよう乱数発生器20で発生した乱数を用いて排他的論理和回路20でスクランブル処理がなされる。この排他的論理和回路20の出力に得られるスクランブル化された放送情報は、契約加入者に対してのみ復号が許可されるが、復号のために必要な情報を放送局側100から加入者側200に伝送する必要がある。

上記したように、放送信号自体は上記擬似ランダム雑音を発生する乱数発生器10の動作により秘匿されるが、どの契約者にどのような番組の視聴を許可するかの復号可能契約者を特定する情報も秘匿する必要がある。このように、番組情報自体を秘匿するための秘匿鍵情報、復号可能契約者を特定するための秘匿鍵情報の2種の暗号鍵としての秘匿鍵情報により有料化がなされる。

このような有料放送システムにおいては、加入者を示す識別符号(ID)、及び予約番組の種類を示すティア(Ti)の公開鍵情報、上記乱数発生器10に対する初期値(In)、上記ティア(Ti)に対する暗号符号であるティアキー(Ki)、上記識別

(7)

符号(ID)に対応するパスワード(Pa)が非公開の暗号鍵として扱われる。

先ず、放送情報を秘匿化する乱数発生器10について述べると、この乱数発生器は例えばM系列符号発生器等で構成され所定のアルゴリズムによる乱数が発生する。この場合乱数発生器10の初期値は同期信号発生回路30で発生するタイミング信号にもとずき、制御回路40の制御のもとにイニシャルデータ発生回路50によって発生する。このイニシャルデータ(In)は上記ティアキー(Ki)とあいまり上記乱数発生器10のシーケンス動作を制御する。

即ち、上記乱数発生器10のシーケンス動作は上記イニシャルデータ(In)とティアキー(Ki)によって制御を受けるわけであるが、上記ティアキー(Ki)は、メモリテーブル60に形成されたチャンネル番号毎に付され番組ジャンルを示すティア(Ti)及びこのティア(Ti)に対して付された暗号ティアキー(Ki)からなるメモリマップより抽出され上記乱数発生器10に与えられる。この結果、上記

(8)

乱数発生器10は、上述の2種類の暗号鍵であるイニシャルデータ(In)、ティアキー(Ki)を用いてKs＝f(In,Ki)なる乱数を発生する。この乱数Ksは一方入力端に放送情報が加えられる排他的論理和回路20の他方入力端に加えられスクランブル化された放送情報が得られる。この場合、上記イニシャルデータ(In)は、スクランブル化された放送情報を平文化するため、暗号鍵情報として用いられるので、イニシャルデータ自体も加入者側にダウンロードされる。

放送局側では、どの加入者がどの番組に対して契約しているかの情報を暗号文として生成するがこの情報もダウンロードして加入者側での復号のための鍵情報(Ei)として用いられる。この暗号情報Eiはメモリテーブル70に形成された各加入者を識別する識別符号(ID)に対応して付された秘匿情報であるパスワード(Pa)と上記ティアキー(Ki)とによりEi＝g(Ki,Pa)として暗号器80で生成される。暗号情報(Ei)も加入者側でスクランブルされた放送情報を復文化するため鍵情報として用い

(9)

られるので、この暗号情報(Ei)を復号できない加入者はスクランブルされた放送情報をディスクランブルして放送信号を受信することはできない。従って、課金マップ90をCPU 110が参照し、CPU 110は料金未納等の契約対象外の者に対しては上記暗号情報(Ei)を作成せず当該加入者は放送の視聴が禁止される。

このように放送局側100からは、第1の鍵情報Ksでスクランブルされた放送情報、契約加入者を特定するに供する第2の鍵情報Ei、及び上記乱数発生器10に対する初期値情報(In)がタイミング回路120によるタイミング制御のもとにモデム130を介して秘匿情報として加入者側120にダウンロードされる。更に、公開鍵である番組属性を示すティア(Ti)がダウンロードされる。

次に、加入者側200についてみると、スクランブルされた放送情報は排他的論理和回路210の一方入力端に加えられる。このスクランブルを解くには、上記乱数発生器10で発生した乱数と同じ乱数を上記排他的論理和回路210の他方入力端に加

(10)

えればよいが、この復号化は上述した第1の鍵情報Ks、第2の鍵情報Eiを生成して乱数発生器220でスクランブル時における乱数と同様の乱数を発生することで行なわれる。このようなディスクランブルに供する乱数を発生するには上記第1の鍵情報を生成する必要があるが、加入者側では第1の鍵情報Ksを再生するためにはティアキー(Ki)、イニシャルデータ(In)を抽出することが必要になる。この場合、ティアキー(Ki)は、ダウンロード時に第2の鍵情報Eiで暗号化されているため、ティアキー(Ki)を直接抽出できず一担第2の鍵情報(Ei)を抽出しこれからティアキー(Ki)を抽出する処理が行なわれなければならない。

ディスクランブル動作を説明するに、先ず、データ処理に必要な同期信号は同期信号抜取り回路221によって抽出され、この同期信号をもとにデータ処理に必要なタイミング信号をタイミング信号発生回路222が発生する。また、放送局側100から送られた関連鍵情報は鍵情報抽出回路223で抽出される。即ち、イニシャルデータ(In)、鍵情

(11)

付されたパスワード(Pa)から上記暗号器80と逆のデータ処理を行ないティアキー(Ki)を生成する。このティアキー(Ki)及び上記鍵情報抽出回路288で抽出したイニシャルデータ(In)をもとに乱数発生器220でスクランブルに供する乱数と同様の乱数が発生する。この乱数は排他的論理和回路210に加えられ、ディスクランブル処理がなされ平文化された放送情報を出力端子ＯＵＴに得る。

これらの一連のディスクランブルに関連するデータ処理はＣＰＵ300による制御による。

次に、契約加入者側200から加入者が放送局側100に対して契約を申し込む場合について述べる。

加入者が契約するには、先ず表示器400に表示された加入者識別符号(ID)をキーパッド400を押釦して入力する。この後、加入者は予じめ知らされている番組態様を示すティア(Ti)を上記キーパッド500を操作して入力し、番組予約を行なう。これらの加入者識別符号(ID)、ティア(Ti)はＣＰＵ300で処理された後にモデム600を介してアップストリームによって放送局側へ送られる。

(13)

報Ei＝g(Ki,Pa)、及びティア(Ti)が鍵情報抽出回路233で上記タイミング発生回路222で規定されるタイミングに従がい抽出される。この抽出された関連鍵情報はＲＡＭ書込制御回路224の制御信号の制御によってＲＡＭ225に書込まれる。このとき、各加入者毎に付されている加入者識別符号(ID)及びパスワード(Pa)が加入者側のＲＯＭ226から読み出されたものと一致しているか否かを比較器227で判別し、比較の結果一致しているときのみ上記ＲＡＭ225に対し関連鍵情報の書き込みが許可される。

また、イニシャルデータ(ID)、公開鍵情報である番組態様を示すティア(Ti)は鍵情報抽出回路228で抽出され上記ＲＡＭ225に書き込まれたティア(Ti)と伝送された番組に付随するティア(Ti)との比較を比較器229で比較を行ない、この比較の結果ティアが一致している場合には制御回路230によって復号器231を動作させる。このとき復号器231は上記ＲＡＭ225から読み出した鍵情報(Ei)と上記ＲＯＭ226から読み出した加入者に

(12)

放送局側100では上記加入者からの予約情報である加入者識別符号(ID)、ティア(Ti)はモデム130で復調された後、課金マップに加入者識別符号(ID)をもとに課金情報を書き込む。そしてＣＰＵ110は上記課金マップ(90)を参照し、料金支払い等を確認した後にメモリテーブル60に対して非公開情報であるティアキー(Ki)を書き込む。これにより予約処理が行なわれ、放能局側100から有料放送情報を入力端子ＩＮから送出する場合には排他的論理和回路20によってスクランブル処理が行なわれた信号が伝送され、加入者側200では契約加入者のみ排他的論理和回路210によってディスクランブルされる。

このように加入者が契約するにあたっては加入者は希望する番組態様に対応した情報であるティア(Ti)を放送局側100に送るわけであるが、加入者が上記ティア(Ti)を放送局側100に予約情報として伝送しないと放送局側100ではデータメモリ60にスクランブル解くための鍵情報の一つであるティアキー(Ki)を書き込まない。このためディス

(10)

クランブルに関係する鍵情報(Ei)が暗号器80で形成されず、また加入者側200でディスクランブルに関連するティアキー(Ki)は生成されない。これは、伝送されたティアキー(Ti)と加入者が設定する予約ティア(Ti)とが一致が比較器229で検出されないことによる。

即ち、加入者が予約をしていないと、上記復号器231はディスクランブルのためのティアキー(Ti)を生成できない。このときディスクランブル動作がなされないことで放送波の視聴ができない加入者は、機器の故障か予約のし忘れによって視聴できないのかの判別できない。

そこで、この実施例では上記比較器229で比較結果をもとにCPU300を制御して、伝送されたティア(Ti)と予約ティア(Ti)とが一致しない場合には、表示器400にティア(Ti)が一致しない旨或は点滅を行なわせて機器の故障によるものではなく予約のし忘れ等によって復号器231が動作していないことによることを加入者に知らせる。

第3図は、第2図に示した実施例において、予

(15)

(Ti)は、加入者が契約したことで放送局側100でメモリテーブル60に契約によってティアキー(Ki)が与えられたティア(Ti)を示す。この予約ティア(Ti)は加入者においては鍵情報抽出回路228によって上記タイミング信号発生回路222で発生するタイミング信号に従がい抽出される。

一方、加入者の契約の有無に拘らず、伝送番組とともに伝送番組の種類を示す信号として機能する受信ティア(Ti)は鍵情報抽出回路228で抽出される。この受信ティア(Ti)は放送情報種別を示す情報として上記予約ティア(Ti)とは異なる情報フレームに挿入して伝送される。

そして、上記鍵抽出回路223で抽出された予約ティア(Ti)はRAM書込制御回路224を介してRAM225に書き込まれる。RAM225に書き込まれた予約ティア(Ti)情報は比較器229の予約ティアレジスタ710に読み出される。また、上記受信ティア(Ti)情報は受信ティアレジスタ720に蓄積され、上記受信ティア、予約ティアの両者が一致しているか否かは比較器229の比較手段730によ

(17)

約ティア(Ti)と受信ティア(Ti)との一致を検出し契約番組か否かの判別を行なう回路の実施例を示す。なお、第2図と同一部分には同一符号を付しその説明を省略する。

第3図において伝送信号中に含まれる同期信号は同期信号抜取り回路221によって抽出され、この抽出された同期信号にもとづいて処理に必要なタイミング信号はタイミング信号発生回路222で発生する。

上記第3図に示した加入者側200では、伝送された鍵情報は鍵情報抽出回路223,228で抽出される。この鍵情報抽出回路228で抽出される鍵情報としてはイニシャルデータ(In)、ティアキー(Ki)と加入者識別符号(ID)に対応して付したパスワード(Pa)から生成した非公開鍵である(Ei)及びティア(Ti)がある。この場合ティア(Ti)は放送局側100から送られるが、加入者が予約を行ない契約した番組であることを示す予約ティア(Ti)と加入者の契約の有無に拘らず伝送される受信ティア(Ti)の2種がある。この2種のうち、予約ティア

(16)

って検出される。即ち、伝送された番組情報が加入者が契約した番組であるか否かの判別が比較器229によってなされる。この場合、予約ティア(Ti)と受信ティア(Ti)が一致していないと、復号器231を制御する制御回路230の制御動作を停止させるとともにCPU300にティア(Ti)の不一致を示す信号を供給する。この信号を受けたCPU300は、表示器400をティアの不一致を示すべく駆動する。

このティアの不一致を示す表示によって、加入者が当該放送情報を視聴できないのは未契約によるものであることが知らされる。

この場合、上記表示器400の表示形態は、例えば全ての番組番号に対して契約済の番組番号を点灯するものであってもよいし、未契約である旨のメッセージを表示する形態、更には番組番号をフラッシングすることで注意を喚起する等種々の形態が適用し得る。

〔発明の効果〕

この発明に係る有料放送方式によれば、上述し

(18)

たように伝送番組に対して加入者が契約しているか否かをスクランブル鍵情報を用いた制御によって加入者に認知させることができる。これにより、加入者は、当該放送が視聴できないのは未契約によることが認識できる。

また、スクランブルを解除するに関与する復号器を上記した未契約番組であるか否かを確認した上で制御するのでスクランブル動作も確実な有料放送方式を提供し得るものである。

4. 図面の簡単な説明

第1図はこの発明に係る有料放送方式の実施例の概要を示す回路図、第2図及び第3図はこの発明に係る有料放送方式の実施例を示す回路図である。

60…番組種別情報発生手段、

70…契約番組種別情報発生手段、

80…鍵情報生成手段、

223,228…抽出手段、

223…鍵情報抽出手段、

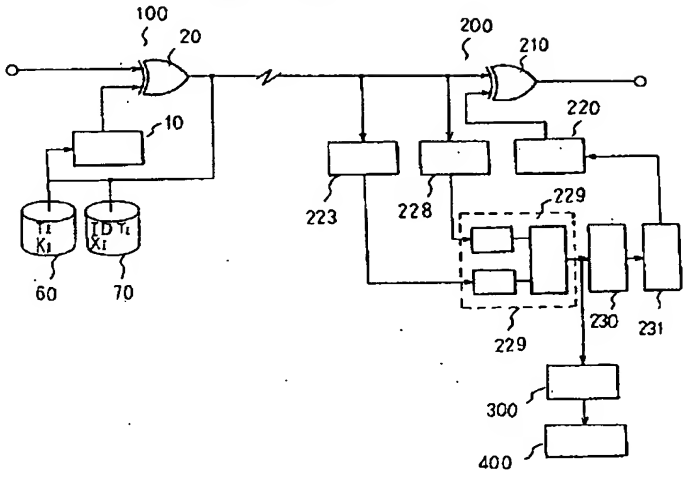
229…比較手段、

400…表示手段。

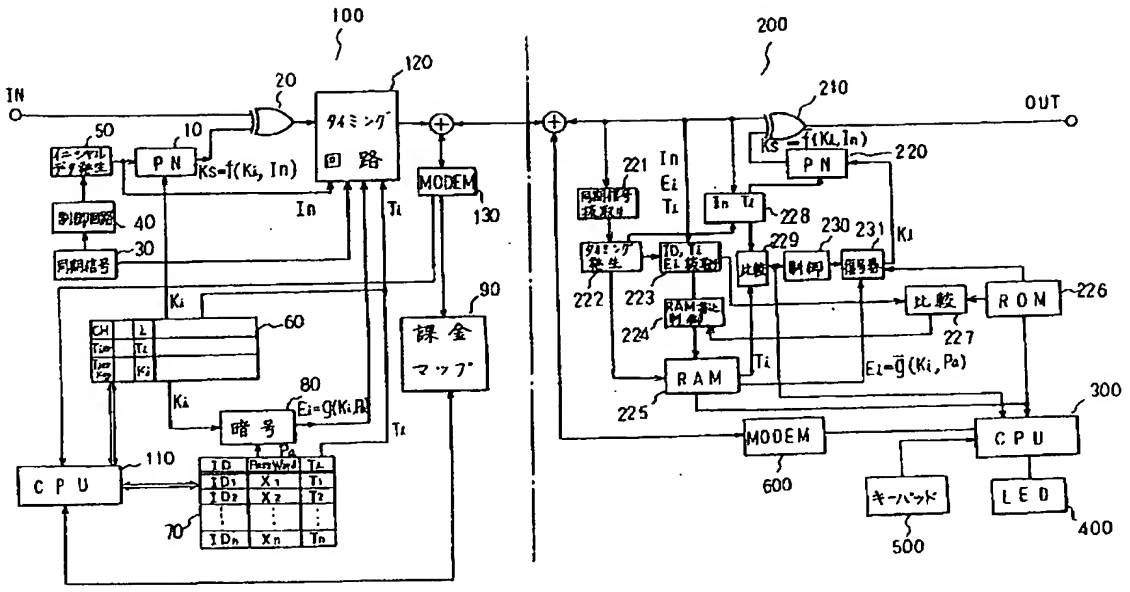
代理人 弁理士 則 近 憲 佑
(ほか1名)

(19) (20)

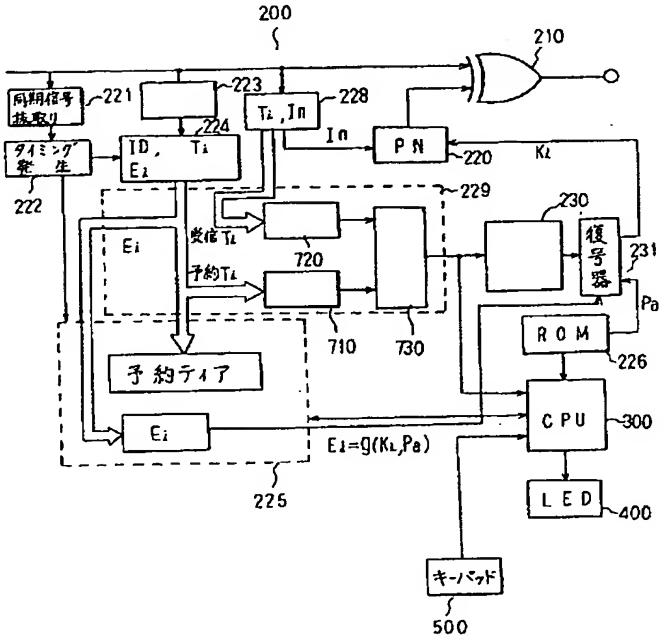
第 1 図



第 2 図


100
200
IN
OUT
20
120
210
50
10
40
30
60
90
80
110
70
130
220
221
222
223
224
225
226
227
228
229
230
231
300
400
500
600
PN
MODEM
CPU
ROM
RAM
LED
Ks=f(Ki, In)
Ei=g(Ki,Pa)
Ks=f(Kl,In)
In
Ti
Ei
Ki
Kl
Pa

第 3 図


200
210
221
223
228
224
222
220
229
230
231
720
710
730
225
226
300
400
500
PN
ROM
CPU
LED
Ti, In
In
Kl
Ei
Pa
予約Ti
予約ティア
Ei=g(Kl,Pa)